$SoNeUCON_{ADM}$: the administrative model for $SoNeUCON_{ABC}$ usage control model

Lorena González-Manzano
Univ. Carlos III de Madrid
lgmanzan@inf.uc3m.es

Ana I. González-Tablas
Univ. Carlos III de Madrid
aigonzal@inf.uc3m.es

José M. de Fuentes
Univ. Carlos III de Madrid
jfuentes@inf.uc3m.es

Arturo Ribagorda
Univ. Carlos III de Madrid
arturo@inf.uc3m.es

***Abstract*—The popularity of Web Based Social Networks (WBSNs) encourages their enhancement. Many WBSN data is considered personal data and access control management plays a key role in this regard. The point is not only to manage access control but to determine how administration should be performed. Based on $SoNeUCON_{ABC}$, an expressive usage control model that allows fine-grained access control management, this paper presents $SoNeUCON_{ADM}$, the complementary administrative model. Based on a pair of related and popular administrative models, the evaluation proves the completeness of $SoNeUCON_{ADM}$.**

***Index Terms*—Administrative access control model, Web Based Social Network, revocation, delegation.**

I. Introduction

In Web Based Social Networks (WBSNs) users upload huge quantity of data, some of them personal data, which are in many cases let out of control. Controlling and carefully managing all WBSNs data is a demanding and challenging necessity. At a primary step, $SoNeUCON_{ABC}$, an expressive usage control model that allows fine-grained access control management along the whole usage process is proposed in [1]. However, access control models have to describe the way administration is performed and then, the identification and specification of administrative tasks for $SoNeUCON_{ABC}$ is the following step.

Coming back to the 90's, given the maturity of the Role Based Access Control Model (RBAC) proposed by R. Shadu *et al.* [2], its attached administrative model can be used as a precedent in the identification of administrative tasks [3]. In a nutshell, in RBAC, administrative permissions (analogous to rights) are exclusively applied to administrative roles and other permissions are applied to any other kind of roles. Then, administrative tasks base on the assignment of users to roles; the assignment of permissions to roles; and the assignment of roles to roles. The initial set of administrative tasks are summarized as follows:

- Who is the entity in charge of creating, updating and deleting access control preferences.
- Who is the entity in charge of associating preferences with data.
- How preferences are associated with data and data with data owners.

Furthermore, administrative issues also involve administrative rights management. Two types of rights are distinguished, namely, use and administrative rights. Use rights consist of operations performed with objects, e.g read right, and administrative rights correspond to operations performed over the right of objects, e.g. the right to give read right. The management of both types of rights is essential and delegation and revocation are remarkable operations in this regard. Delegation focuses on granting a right to a user, while revocation undoes the effects of delegation. In particular, *weak* and *strong revocation* are differentiated. The former refers to simply remove granted permissions and the latter refers to recursively revoke permissions from those to whom the grantee granted the permissions. Based on these rights and operations, the following administrative tasks are added to the previous ones:

- Who is the entity in charge of managing revocation.
- Who is the entity in charge of managing delegation.
- How weak and strong revocation is managed based on use rights and administrative rights.
- How delegation is managed based on use rights and administrative rights.

In the social networking field administration focuses on managing uploaded resources like photos or videos, specified identity data (namely personal profiles) and established access control policies. Thus, WBSN administrative tasks are equivalent to the ones above mentioned but considering that resources, identity data and policies are the elements at stake. As a result, this paper presents $SoNeUCON_{ADM}$, an administrative model for $SoNeUCON_{ABC}$. $SoNeUCON_{ADM}$ addresses all aforementioned tasks to promote a wider use of $SoNeUCON_{ABC}$.

This paper is structured as follows. Related work is described in Section II. Section III presents the background. Section IV introduces administrative features, particularly, tasks and rights. In Section V $SoNeUCON_{ADM}$ is described. The evaluation of the model is described in Section VI. Lastly, conclusions and future work is outlined in Section VII.

II. Related work

This Section presents the analysis of 21 proposals in the literature that address administrative issues in collaborative environments. Note that this study is not exclusively focused on WBSNs, but extended to collaborative environments due to a pair of reasons. On the one hand, WBSNs manage data which may be related to multiple users and then, they can be pointed out as collaborative systems. On the other hand, a

ISBN: 978-84-9717-323-0

TABLE I
ADMINISTRATIVE FEATURES ANALYSIS

	Proposals	Administration	Delegation	Revocation
[25]	B. Carminati et al. (2011)	D		
[6]	A.C. Squicciarini et al. (2009)	D		√*
[24]	H. Zhang et al. (2012)	C		
[5]	M.R. Thompson et al. (2003)	D	√	√
[7]	A.C. Squicciarini et al. (2010)	D		√*
[8]	A. Ahmad et al. (2012)	D	√	√
[9]	Y. Jung et al. (2013)	D		√
[10]	Y. Ren et al. (2011)	D		
[11]	M. Prilla et al. (2006)	D		√
[12]	A. Imine et al. (2009)	D		√
[13]	M. Lorch et al. (2003)	D	√	√
[14]	H.F. Wedde et al. (2003)	D		
[15]	R. S. Shandu et al. (2010)	D	√	√
[16]	R. S. Shandu et al. (2011)	D	√	√
[17]	W.K. Edwards (1996)	C		
[18]	K. Sikkel et al. (1997)	D	√	√
[19]	Z.Y. Zhang et al. (2011)	D	√	√
[20]	R.K. Thomas (1997)	C		
[21]	E. Cohen et al. (2002)	D	√*	
[22]	V. Gligor et al. (2002)	D		√*
[23]	J. Jin et al. (2006)	D	√	

∗: mentioned but not managed

small amount of proposals focus on administrative issues in the specific context of WBSNs.

In general, 6 contributions fall in the WBSN category [4], [5], [6], [7], [8], [9], 3 proposals in document sharing [10], [11], [12], one proposal bases on grid environments [13] and the rest of them focus on other general collaborative systems [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24].

This analysis studied the administration type, namely, centralized C (a single entity decides who can get into the systems) or decentralized D (multiple entities decide who can get into the systems); and how delegation and revocation are managed. Table I presents results of the analysis. Symbol * means that a particular feature has been mentioned but not managed.

In what concerns the administration type, 18 approaches deal with D administration and just 3 proposals focus on C administration. As expected, administration tends to be decentralized because each WBSN user has to manage his owned data.

Concerning centralized administration, in [17] a central administrator manages roles and policies. Furthermore, the need of dynamism is highlighted and the change of user roles, at runtime, is an essential matter to deal with. Similarly, [20] proposes teams management. Teams are composed of users with the same role whose management is left to a general administrator. Likewise, in [24] groups are managed by a central authority in such a way that users are added to groups and rules, based on user attributes, time periods and resource usages, are applied to groups.

The majority of approaches base on decentralized administration, allowing users to individually manage their personal data. For instance, in [12], the administrators initiate the administration process by notifying updates to affected users who become involved in the administrative management process. By contrast, in [23], [5] users who want to become involved in a particular administrative process have to request it. Other proposals divide data, particularly documents, among users and they work over each owned piece of data [10]. A different solution are proposed by M.R. Thompson *et al.* [5] and A. Ahmad *et al* [8]. M.R. Thompson *et al's* work bases on certificates jointly signed by all users involved in the administrative process. However, A. Ahmad *et al* propose *transfer*, *multiplication* and *division* operations [8].

Delegation, associated with decentralized administration, is addressed in a total of 9 approaches. In collaborative environments several users have to cooperate to achieve a common goal. Then, delegating permissions breaks the power of a central administrative user by sharing administrative tasks among different parties. The most of approaches focus on permissions delegation [15], [16], [18], [13], [5], [24], [8], being the proposals of Z.Y. Zhang *et al.* and J. Jin [23] the only ones which propose role delegation [19] and E. Cohen *et al.*'s proposal which exclusively mentions the difficulty in managing delegation in organizational environments [21].

Related to revocation management, in multiple cases users may regret having granted a certain use or administrative right to a user. A total of 10 proposals provide mechanisms to deal with revocation and other 3 contributions mention the relevance of its management [22], [6], [7]. They focus on weak revocation in respect to rights [15], [16], [11], [13], [8] and group memberships [12] and on strong revocation regarding delegated rights [18], [19], [9] and certificates [5].

In sum, it is concluded that administration in collaborative environments tends to be decentralized. This is specially remarkable in WBSNs, where many users and data are managed. Besides, most of analysed approaches propose revocation and delegation mechanisms which helps to conclude the relevance of their management as part of the administration process.

III. BACKGROUND: $SoNeUCON_{ABC}$

$SoNeUCON_{ABC}$ is an expressive usage control model that manages six WBSN features, namely, common-contacts, clique, distance, multi-path, direction and flexible attributes [26], [27], [28], [29].

In general, $SoNeUCON_{ABC}$ is composed of seven elements: *Subjects* (S) together with *Subject attributes* ($ATT(S)$) refer to WBSN users and their attributes; *Objects* (O) together with *Object attributes* ($ATT(O)$) correspond to WBSN data and their attribute; and *Relationships* (RT) together with *Relationship attributes* ($ATT(RT)$) refer to the set of relations and attributes that exist between a pair of users, being direct relationships denoted as E and $ATT(E)$ their attached attributes; *Rights* (R) correspond to actions that can be performed over objects O; *Authorizations* (A) refer to rules to satisfy to grant a subject a right on an object; *Obligations* (B) correspond to requirements to satisfy before or while the usage process; and *Conditions* (C) refer to requirements to satisfy in regard to context features, eg. network availability.

In $SoNeUCON_{ABC}$, access control policies, denoted as ρ, consist of $\rho(\rho_s; \rho_o; \rho_{rt}; r; \partial_b; \partial_c)$. In particular, ρ_s, ρ_o and ρ_{rt} are predicates defined over subject, object and relationship attributes respectively. Besides, rights are denoted as r and obligations and conditions refer to ∂_b and ∂_c respectively.

In the following, an example of an access control policy is presented: *Access is granted to photos entitled "Party" to friends of a friend if they are under 30 years old or if they are under 25 years and have studied computer science.*

$\rho = (((age < 30) \vee ((age < 25) \wedge (studies = c.science)))$; $(title = party)$; $((((role = friend)$; $(role = friend))), \emptyset, \emptyset)$; $read$; $\emptyset$; $\emptyset)$

For more details of $SoNeUCON_{ABC}$ usage control model see [1].

IV. Towards administration

Prior to the description of how administration is performed in $SoNeUCON_{ADM}$, administrative tasks to address (Section IV-A) and the available rights to manage (Section IV-B) are detailed in the following Sections.

A. Administrative tasks

Administration involves multiple tasks (recall Section I) which can be classified in a couple of groups regarding tasks related to:

- *The identification of who is involved in administrative issues*. These tasks refer to who manages access control policies, who associates policies with resources and identity data and who manages revocation and delegation.
- *The definition of how administrative issues are performed*. These tasks correspond to how policies are associated with resources and identity data, how resources and identity data are associated with their owners and how revocation and delegation are managed.

B. Rights management

Two types of rights are differentiated, *use rights* and *administrative rights*. The former ones, which are referred in $SoNeUCON_{UCON}$ to as Rights (R), base on operations performed with objects such as read, and operations carried out over objects like tag, move or copy. By contrast, *administrative rights* (AR) refer to the management of elements involved in the access control decision process, along with delegation and revocation management.

V. $SoNeUCON_{ADM}$ definition

Users enrolled in a WBSN become owners of uploaded resources, established identity data (mainly profile data) and defined access control policies. Thus, $SoNeUCON_{ADM}$ is based on **ownership**, such that owned elements are managed by their owners. Specifically, administrative objects (AO) correspond to the elements involved in the access control decision process, namely, managed subjects (S), objects (O), direct relationships (E) and their respective attributes ($ATT(S)$, $ATT(O)$,$ATT(E)$) and access control policies (ACP).

In $SoNeUCON_{ADM}$, owners execute administrative rights AR over administrative objects AO and grant use rights R over objects O according to access control policies ACP (see Figure 1). In this regard, following Sections describe use rights R and administrative rights AR management (Section V-A and V-B respectively).

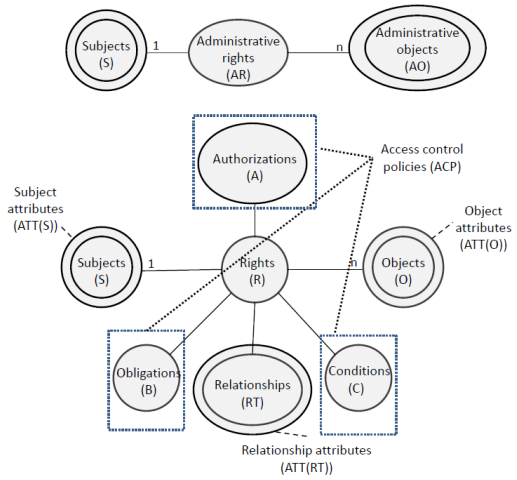

Fig. 1. $SoNeUCON_{ADM}$

A. Use rights management

Each owner specifies as many access control policies as desired and leaves them in a pool of policies to be evaluated when a request is received for executing some right over one of his owned objects. Contrary to other models, policies in ACP are not directly associated with data and its owner but to the owner exclusively. For instance, the policy "*grant read access to data entitled PARTY to users older than 20*" is created, associated with an owner and located in his pool of policies. Next, when an object of a particular owner is requested, all policies associated with him are evaluated, verifying authorizations (A), composed of subjects, objects and relationship attributes and the granted right ($ATT(S)$, $ATT(O)$, $ATT(RT)$ and r), obligations (∂_b) and conditions (∂_c). If there is a policy ρ_i within the set of policies defined by an owner (P_{ow_i}) that matches the request, the right r over the requested object o is granted to the requester s. Assuming that the expression $owner(\text{"}element\text{"})$ means being owner of "element", it is formally defined as:

(s, o, r) $granted \Leftarrow P_{ow_i}$= $\{\rho_i \in ACP / owner(\rho_i) = owner(o)\} \wedge$
$\exists \rho_i (A(ATT(S), ATT(O), ATT(RT), r); \partial_b; \partial_c) \in P_{ow_i} /$
$\rho_i (A(ATT(s), ATT(o), ATT(rt(owner(o), s)), r); \partial_b; \partial_c) = true$

B. Administrative rights management

This Section details the management of administrative objects (AO), revocation and delegation. In general, being owner of a particular administrative object ao grants administrative rights AR over it to manage the object and its attributes and to delegate and revoke use rights R and administrative rights AR over it. It is formally defined as:

$(s, ao, management)$ granted$\Leftarrow s = owner(ao)$
$(s, ao, delegation)$ granted$\Leftarrow s = owner(ao)$
$(s, ao, revocation)$ granted$\Leftarrow s = owner(ao)$

1) Administrative objects management: Administrative objects AO management consists of the creation, modification and deletion of any AO.

In terms of subjects S, they can create WBSN accounts, becoming owners of their profiles, uploaded data and established access control policies. Analogous, they can cancel their accounts whenever desired.

Objects O are other topic for discussion. In general, objects are stored in WBSN data bases, eg. Facebook. Nonetheless, in decentralized WBSNs, like Diaspora, each user chooses the host to store his data. Similar to WBSN accounts, objects have to be deleted when users want.

In regard to direct relationship E (as the indirect once are constructed through them [1]), WBSN users establish relationships with other users, as well as they update or remove them.

Concerning attributes, subject, objects and relationships attributes have to be considered ($ATT(S)$, $ATT(O)$ and $ATT(E)$ respectively). Firstly, $ATT(S)$ which basically refer to profile data, are linked to a WBSN account and they can be established by the account's owner, retrieved from an Identity Provider (IdP) where they where previously defined or obtained from personal devices like identity cards. Second, $ATT(O)$ attached to an object can be defined by its owner, as well as retrieved from the object's metadata. Nonetheless, if required, owners have to give permission to WBSNs to process metadata. Finally, what concerns with $ATT(E)$, they are considered identity data and then, they can be defined by owners or retrieved from IdPs.

On the other hand, access control policies can be also created, updated or deleted, at any time. In particular, all subjects with a WBSN account can manage access control policies ACP.

One last point is that the use of attributes, conditions and obligations in spite of being opened sets, depends on what every WBSN supports.

2) Delegation management: Delegations consist of granting permission to a certain user over a particular object temporary or permanent. The delegation of use rights R can be analogous to the establishment of access control policies. A right is granted to the requester over the requested object after satisfying an access control policy.

On the contrary, the delegation of AR requires the definition of the following function:

- DELEGATE(v_k,v_j,o_i,λ): It states that v_k gives a specific AR λ to v_j over o_i. λ refers to a partial or a complete delegation, the former to delegate some AR and the latter to delegate all AR. λ takes the value $*$ for a complete delegation and takes the value, e.g., AR-R to express that only the permission to grant use rights R is delegated. Note that this administrative model applies permanent delegation and the temporal one is left as a matter of future work.

In $SoNeUCON_{ADM}$ the delegation of AR compels the permanent delegation of all AR. Thus, the object over which the operation is executed, becomes property of the delegatee. The delegation operation should be enforced such as λ takes the value $*$, DELEGATE(v_k,v_j,o_i,$*$).

3) Revocation management: Revocation, contrary to delegation, removes the granted right over an object to a certain user. There are two types of revocation, weak and strong (Section I). Nonetheless, weak revocation of use rights R is the only $SoNeUCON_{ADM}$ manages since the delegation of AR is permanent and recursive delegation of use rights R are not applied.

$SoNeUCON_{ADM}$ manages revocation in terms of the update of attributes and access control policies, eg. if a photo entitled "Summer" is accessible to relatives, it would remain accessible to this set of people until the policy or the photo's title change. Indeed, it is extremely related to usage control and the application of *mutability* and *continuity* attributes. *Mutability* refers to the fact that attributes can be updated at any time. On the other hand, *continuity* refers to the enforcement of access control along the whole usage process. Both attributes are directly related to revocation because if initial conditions change along the usage process, access decisions have to be taken again [30] and they may cause the revocation of granted rights. Based on [31], revocation can be also divided between direct and indirect:

- *Direct revocation* can be enforced, at any time, by the owners of resources and identity data. Data owners may decide to revoke rights previously granted, updating or deleting an access control policy, as well as changing attributes. For instance, if the right to access a photo entitled "Classes" is granted to relationships with role "classmates", revocations can be caused by the update of the title of the photo or by the update of the role of a classmate relationship. Likewise, if the policy " Grant access to Friends to all photos" is updated to "Grant access to Friends to photos entitled Birthday", it may prevent requesters from getting requested rights in subsequent requests or while the usage process.
  In the revocation process, apart from the data owner, the Usage Reference Monitor is the entity at stake. This entity is composed of a Usage Decision Facility (UDF) and a Usage Enforcement Facility (UEF) which are always active [34] and they are applied in the usage control process. UDF identifies changes in attributes and UEF enforces access control accordingly. When policies are updated or attributes are changed, the UDF is informed about that. Afterwards, it informs the occurred event to the UEF and lastly, the UEF enforces the re-evaluation of policies.
- *Indirect revocation* is caused by uncontrolled situations. Particularly, it is performed when access control policy attributes expire or change. "Automatic" attributes updates, either subjects, objects or relationship attributes, can cause revocation of granting rights."Automatic' means that no users interactions are required. For instance, if the right to access a photo entitled "High-school" is granted to users under 18, revocations occur when requesters turn to 18 years old. Note that "automatic" updates are

TABLE II
ADMINISTRATIVE TASKS COMPARISON

Tasks	**SoNeUCON**_ADM	**UCON**_ABC [32], [33]	**RBAC** [3]
Entities identification			
Creating, updating and deleting access control preferences	Owners.	Owners.	Owners.
Associating preferences to data	Not required	-	Owners
Revocation management	Usage reference monitor and owners	-	Owners
Delegation management	Owners	-	Owners
Management procedures			
Association between preferences with data and data with data owners	Policies are exclusively associated to data owners concerning subjects, objects and relationships attributes.	Assertions associate subjects and objects	Permissions are associated with roles and and data and roles with data owners
Revocation management	Weak revocation is managed. Attributes and access control policies updates.	Weak revocation is managed. Time assigned to access control policies.	Weak and strong revocation are managed. Owners revoke users from roles according to their decisions.
Delegation management	Delegation of R and all AR is available. Owners establish access control policies and execute the delegation operation for all AR.	Delegation of R. Assertions associated with particular requesters.	Delegation of R and AR is available. Owners assigned users to roles to delegate.

specially related to attributes in which time is directly or indirectly involved.

The management is equivalent to *direct revocation* except for the fact that the UDF identifies updated attributes.

VI. EVALUATION

This Section presents the evaluation of $SoNeUCON_{ADM}$, the administrative model for $SoNeUCON_{ABC}$. It consists of comparing the proposed model with the most challenging and related administrative models, RBAC and $UCON_{ABC}$. $SoNeUCON_{ADM}$ is compared with RBAC administrative model, for being one of the most mature administrative models [35], [3], and with $UCON_{ABC}$ administrative capabilities, for being the model that lays the bases on the proposed one [32], [33].

Administrative tasks, identified in Section I, are depicted and compared in Table II, where symbol '-' implies that a particular task is not studied.

Concerning the association of data with preferences and data with data owners, $SoNeUCON_{ADM}$ only requires to associate preferences (access control policies) to data. Policies are mainly defined over subjects, objects and relationships attributes instead of being attached to specific objects. By contrast, $UCON_{ABC}$ and RBAC pose more restrictive and tedious tasks from the users point of view. In $UCON_{ABC}$ owners define assertions to associate subjects with objects, as well as to associate policies (composed of assertions) with objects [33]. However, in RBAC permissions are assigned to roles and to objects and then, roles are assigned to users.

Delegation is also managed in all compared models, being the $SoNeUCON_{ADM}$ proposal the most flexible one. In $SoNeUCON_{ADM}$ delegating R involves the establishment of access control policies according to subjects, objects and relationship attributes. Moreover, the delegation of all AR involves the execution of the operation DELEGATE to guarantee that, from the moment the operation is enforced, the delegated object becomes property of the delegatee without the possibility of undoing the operation. Conversely, delegation in $UCON_{ABC}$ is limited to R. It bases on specifying assertions associated with particular requesters which base on objects and subjects attributes [33]. On the other hand, RBAC delegates R and AR through the association of roles to users.

Revocation is another compared task. $SoNeUCON_{ADM}$ manages direct and indirect revocation. The former is performed by owners through the change of attributes and access control policies. On the contrary, indirect revocation is exclusively related to attributes updates, being particularly related to attributes involving time restrictions. Nonetheless, as this model only delegates R and all AR, just weak revocation is at stake. Similarly, $UCON_{ABC}$ manages weak revocation assigning time to access control policies. Moreover, though not described in the original model, Z. Zhang *et al.* proposed a general procedure to manage weak and strong revocation in $UCON_{ABC}$ [36]. On the other hand, RBAC provides functions to weakly and strongly revoke users from roles by removing the assignment of users to roles.

In the light of the proposed analysis, $SoNeUCON_{ADM}$ supports all tasks an administrative model should provide and thus, their completeness is pointed out. Indeed, $SoNeUCON_{ADM}$ has a significant advantage, that is, preferences (access control policies) are associated to users instead of to objects and the burden of managing at least as many policies as uploaded objects is avoided. Moreover, it is noticeable that $SoNeUCON_{ADM}$ does not manage strong revocation because cascading delegations are not required. In other words, this model bases on ownership and then, owners should manage access control in regard to data their posses, either being an entire piece of data or, when co-ownership management takes place, a part of it.

VII. CONCLUSIONS

In this paper, $SoNeUCON_{ADM}$, the administrative model for $SoNeUCON_{ABC}$ usage control model, has been proposed. It supports administrative tasks concerning the identification of who is involved in administrative issues and how they are performed. $SoNeUCON_{ADM}$ has been assessed against a pair of administrative access control models (RBAC and $UCON_{ABC}$) to ensure that it successfully addresses all identified administrative tasks.

In what concerns $SoNeUCON_{ADM}$, the main future step is the management of temporal delegations. Moreover, its

implementation either in a real or in a simulated environment is expected in future work to prove the feasibility of its implementation and the study of users satisfaction.

REFERENCES

[1] L. González−Manzano, A. I. González−Tablas, J. M. de Fuentes, and A. Ribagorda, "SoNeUCON$_{ABC}$, an expressive usage control model for Web-Based Social Networks," *Computers & Security, In Press*, 2014.

[2] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38 –47, 1996.

[3] R. Sandhu, V. Bhamidipati, and Q. Munawer, "The arbac97 model for role-based administration of roles," *ACM Trans. Inf. Syst. Secur.*, vol. 2, no. 1, pp. 105–135, 1999.

[4] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "A semantic web based framework for social network access control," in *Proceedings of the 14th ACM symposium on Access control models and technologies*, ser. SACMAT '09. ACM, 2009, pp. 177–186.

[5] M. Thompson, A. Essiari, and S. Mudumbai, "Certificate-based authorization policy in a pki environment," *ACM Trans. Inf. Syst. Secur.*, vol. 6, no. 4, pp. 566–588, 2003.

[6] A. Squicciarini, M. Shehab, and F. Paci, "Collective privacy management in social networks," in *Proceedings of the 18th international conference on World wide web*, ser. WWW '09, 2009, pp. 521–530.

[7] A. Squicciarini, M. Shehab, and J. Wede, "Privacy policies for shared content in social network sites," *The VLDB Journal*, vol. 19, no. 6, pp. 777–796, 2010.

[8] A. Ahmad, B. Whitworth, and L. Janczewski, "More choices, more control: Extending access control by meta-rights reallocation," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, 2012, pp. 1113 –1118.

[9] Y. Jung and J. Joshi, "Cpbac: Property-based access control model for secure cooperation in online social networks," *Computers & Security*, 2013.

[10] Y. Ren, "Access control in a cooperative editing system," in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, 2011, pp. 77 –80.

[11] M. Prilla and C. Ritterskamp, "Collaboration support by co-ownership of documents," in *Proceedings of the 2006 conference on Cooperative Systems Design: Seamless Integration of Artifacts and Conversations – Enhanced Concepts of Infrastructure for Communication*, 2006, pp. 255–269.

[12] A. Imine, A. Cherif, and M. Rusinowitch, "A flexible access control model for distributed collaborative editors," in *Proceedings of the 6th VLDB Workshop on Secure Data Management*, ser. SDM '09, 2009, pp. 89–106.

[13] M. Lorch, D. B. Adams, D. Kafura, M. S. R. Koneni, A. Rathi, and S. Shah, "The PRIMA System for Privilege Management, Authorization and Enforcement in Grid Environments," in *Proceedings of the 4th International Workshop on Grid Computing*, ser. GRID '03. IEEE Computer Society, 2003, pp. 109–.

[14] H. Wedde and M. Lischka, "Cooperative role-based administration," in *Proceedings of the eighth ACM symposium on Access control models and technologies*. ACM, 2003, pp. 21–32.

[15] R. Sandhu, R. Krishnan, J. Niu, and W. Winsborough, "Group-centric models for secure and agile information sharing," *Computer Network Security*, pp. 55–69, 2010.

[16] R. Sandhu, K. Bijon, X. Jin, and R. Krishnan, "Rt-based administrative models for community cyber security information sharing," in *CollaborateCom*, 2011, pp. 473–478.

[17] W. Edwards, "Policies and roles in collaborative applications," in *Proceedings of the 1996 ACM conference on Computer supported cooperative work*, ser. CSCW '96. ACM, 1996, pp. 11–20.

[18] K. Sikkel, "A group-based authorization model for cooperative systems," in *Proceedings of the fifth conference on European Conference on Computer-Supported Cooperative Work*, ser. ECSCW'97. Kluwer Academic Publishers, 1997, pp. 345–360.

[19] Z. Zhang, T. Huang, Q. Wu, and J. Pu, "A cscw-enabling integrated access control model and its application," *Key Engineering Materials*, vol. 460, pp. 96–105, 2011.

[20] R. Thomas, "Team-based access control (tmac): a primitive for applying role-based access controls in collaborative environments," in *Proceedings of the second ACM workshop on Role-based access control*, ser. RBAC '97. ACM, 1997, pp. 13–19.

[21] E. Cohen, R. Thomas, W. Winsborough, and D. Shands, "Models for coalition-based access control (cbac)," in *SACMAT*, 2002, pp. 97–106.

[22] V. Gligor, H. Khurana, R. Koleva, V. Bharadwaj, and J. Baras, "On the negotiation of access control policies," in *Security Protocols*. Springer, 2002, pp. 188–201.

[23] J. Jin and G.-J. Ahn, "Role-based access management for ad-hoc collaborative sharing," in *Proceedings of the eleventh ACM symposium on Access control models and technologies*, ser. SACMAT '06. ACM, 2006, pp. 200–209.

[24] H. Zhang, W. Wu, and Z. Li, "Open social based group access control framework for e-science data infrastructure," in *E-Science (e-Science), 2012 IEEE 8th International Conference on*. IEEE, 2012, pp. 1–8.

[25] B. Carminati, E. Ferrari, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "Semantic web-based social network access control," *computers & security*, vol. 30, no. 2, pp. 108–115, 2011.

[26] P. W. Fong and I. Siahaan, "Relationship-based access control policies and their policy languages," in *Proceedings of the 16th ACM symposium on Access control models and technologies*, ser. SACMAT '11. ACM, 2011, pp. 51–60.

[27] Y. Cheng, J. Park, and R. Sandhu, "Relationship-Based Access Control for Online Social Networks: Beyond User-to-User Relationships," in *SocialCom*, 2012, pp. 646–655.

[28] B. Carminati, E. Ferrari, and A. Perego, "Rule-Based access control for social networks," in *Proceedings of the 2006 international conference on On the Move to Meaningful Internet Systems: AWeSOMe, CAMS, COMINF, IS, KSinBIT, MIOS-CIAO, MONET - Volume Part II*, ser. OTM'06. Springer-Verlag, 2006, pp. 1734–1744.

[29] B. Carminati and E. Ferrari, "Access control and privacy in web-based social networks," in *International Journal of Web Information Systems*, no. 4, 2008, pp. 395–415.

[30] A. Lazouski, F. Martinelli, and P. Mori, "Usage control in computer security: A survey," *Computer Science Review*, vol. 4, no. 2, pp. 81 – 99, 2010.

[31] N. Attrapadung and H. Imai, "Attribute-based encryption supporting direct/indirect revocation modes," in *Cryptography and Coding*. Springer, 2009, pp. 278–300.

[32] J. Park, "Usage Control: A Unified Framework for Next Generation Access Control," Ph.D. dissertation, George Mason University, 2003.

[33] F. Salim, J. Reid, and E. Dawson, "An administrative model for UCON$_{ABC}$," in *Proceedings of the Eighth Australasian Conference on Information Security*, ser. AISC '10, 2010, pp. 32–38.

[34] R. Sandhu and J. Park, "Usage control: A vision for next generation access control," *Computer Network Security*, pp. 17–31, 2003.

[35] J. Crampton and H. Khambhammettu, "Delegation in role-based access control," in *Computer Security–ESORICS 2006*. Springer, 2006, pp. 174–191.

[36] Z. Zhang, L. Yang, Q. Pei, and J. Ma, "Research on usage control model with delegation characteristics based on om-am methodology," in *Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on*. IEEE, 2007, pp. 238–243.